AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Western District of Texas

FILED
2012 MAR 21 PM 2:08
CLERK US DISTRICT COURT
WESTERN DISTRICT OF TEXAS
BY _____ DEPUTY

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Facebook Account: "Eric Makesumoutofnuttin Carter"
Facebook UID: 155832940

Case No. 1:12-m-183

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

SEE AFFIDAVIT OF SA ANDREW DOOHER

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT "A"

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 USC 871	Threats to the President of the United States
18 USC 844(e)	Bomb Threats

The application is based on these facts:

SEE AFFIDAVIT OF SA ANDREW DOOHER

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

A.M. Dooh
Applicant's signature

SA Andrew M. Dooher, USSS
Printed name and title

Sworn to before me and signed in my presence.

Date: 3/21/12

Judge's signature

City and state: Austin, Texas

Dennis G. Green U.S. Magistrate Judge
Printed name and title

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

IN RE SEARCH OF:	
FACEBOOK ACCOUNTS:	CASE NO. 1:12-m-183
"John Jones" Facebook UID: 100002926201234	1:12-m-186
And	
"Eric Makesumoutofnuttin Carter" Facebook UID: 155832940	

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Andrew Dooher, being duly sworn, hereby state the following under penalty of perjury:

1. I am a Senior Special Agent with the United States Secret Service and have been so employed for over twenty years. I am currently assigned to the Austin, Texas, Resident Office. In this capacity, I have received extensive training and have experience in conducting investigations related to individuals and groups who made threats to the President of the United States and other protectees of the United States Secret Service.

2. This affidavit is submitted in support of an application for a search warrant for a certain accounts controlled by Facebook.com Online Services ("Facebook"), headquartered at 18 Hacker Way, Menlo Park, CA 94025. The accounts to be searched are:

"John Jones"
UID: 100002926201234
http://facebook.com/profile.php?id=100002926201234

and

"Eric Makesumoutofnuttin Carter"
UID: 155832940
http://facebook.com/profile.php?id=1558326940

3. The statements contained in this Affidavit are based on my experience and background as a Special Agent and on information provided by other law enforcement agents. I have not set forth every fact resulting from the investigation; rather, I have included only that information necessary to establish probable cause to conduct a search of the Target Accounts for evidence related violations of Title 18, United States Code, Section 871(a), Threats Against the President and Successors to the President, and Title 18, United States Code, Section 844(e), Bomb Threats.

4. For the reasons set forth below, I respectfully submit that this affidavit contains probable cause to believe that the Target Account will contain evidence that will assist in the investigation and prosecution John Peter Bateman, for violations of Title 18, United States Code, Sections 871(a) and 844(e).

STORED WIRE AND ELECTRONIC COMMUNICATION ACCESS

5. Title 18, United States Code, Chapter 121, Sections 2701 through 2711, is entitled "Stored Wire and Electronic Communications and Transactional Records Access."

a. Title 18, United States Code, Section 2703(a) provides, in part:

> A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has

been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

b. Title 18, United States Code, Section 2703(b) provides, in part:

> (1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection—
>
> > (A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure or equivalent State warrant . . . .
>
> (2) Paragraph (1) is applicable with respect to any electronic communication that is held or maintained on that service—
>
> > (A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and
> >
> > (B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

c. The government may also obtain records and other information pertaining to a subscriber to or customer of electronic communication service or remote computing service by way of a search warrant. 18 U.S.C. § 2703(c)(1)(A). No notice to the subscriber or customer is required. 18 U.S.C. § 2703(c)(3).

d. Title 18, United States Code, Section 2711, provides, in part:

> As used in this chapter—
>
> (1) the terms defined in section 2510 of this title have, respectively, the definitions given such terms in that section; and

(2) the term "remote computing service" means the provision to the public of computer storage or processing services by means of an electronic communications system.

e. Title 18, United States Code, Section 2510, provides, in part:

(8) "contents," when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication; . . .

(14) "electronic communications system" means any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications; . . .

(15) "electronic communication service" means any service which provides to users thereof the ability to send or receive wire or electronic communications; . . .

(17) "electronic storage" means—

(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and

(B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication.

BACKGROUND REGARDING COMPUTERS, THE INTERNET, AND E-MAIL

6. The term "computer" as used herein is defined in 18 U.S.C. § 1030(e)(1), and includes an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

7. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience and knowledge, I know the following:

a. The Internet is a worldwide network of computer systems operated by governmental entities, corporations, and universities. In order to access the Internet, an individual computer user must subscribe to an access provider, which operates a host computer system with direct access to the Internet. The world wide web ("www") is a functionality of the Internet which allows users of the Internet to share information;

b. With a computer connected to the Internet, an individual computer user can make electronic contact with millions of computers around the world. This connection can be made by any number of means, including modem, local area network, wireless and numerous other methods; and

c. E-mail is a popular form of transmitting messages and/or files in an electronic environment between computer users. When an individual computer user sends e-mail, it is initiated at the user's computer, transmitted to the subscriber's mail server, then transmitted to its final destination. A server is a computer that is attached to a dedicated network and serves many users. An e-mail server may allow users to post and read messages and to communicate via electronic means.

SERVICES PROVIDED BY FACEBOOK

8. Based on my training and experience and the experience and training of other law enforcement officers with whom I have had discussions, I have learned the following about Facebook:

a. Facebook provides content services to Internet users. Subscribers obtain an account by registering with Facebook. Facebook requests that subscribers

provide basic information, such as name, gender, zip code and other personal/biographical information. In general, Facebook does not verify all of the information provided, although Facebook will verify email addresses and cellular phone numbers.

b. Facebook maintains electronic records pertaining to the individuals and companies for which it maintains subscriber accounts. These records include account access information, information regarding messages sent or received by the account, and account application information;

c. Facebook subscribers may access their accounts on servers maintained and/or owned by Facebook by using a modem or from any computer connected to the Internet located anywhere in the world;

d. When the subscriber sends a message, it is initiated at the user's computer, transferred via the Internet to Facebook's servers, and then transmitted to its destination.

e. A Facebook subscriber can store files, including messages and image files, on servers maintained and/or owned by Facebook;

f. Facebook maintains a user basic subscriber information (BSI) which may include a subscriber's user identification number, a subscriber's email address, a date/time stamp of account creation, a subscriber's most recent logins, a subscriber's registered mobile phone number and verification on whether the subscriber account is publicly viewable.

g. Facebook maintains a user Neoprint which may include a subscriber's profile contact information, mini-feed, status updates, shares, notes, wall postings, a

friends listing (with Friends Facebook ID), groups listing (with Friends Facebook ID), a subscriber future and past events and a subscriber's video listing.

h. Facebook maintains user photoprints which is a compilation of all photos uploaded by the subscriber and photos that were uploaded by other users in which the subscriber was "tagged".

i. Facebook maintains private messages that have been sent and received.

j. Facebook maintains Internet Provider logs to include access date and time.

PROBABLE CAUSE TO SEARCH THE TARGET ACCOUNTS

9. *EC* is a real person with a date of birth of *xxxxxx* and resides at 6702 *SD* in Austin, TX. *EC* utilizes the email address L*xxxxxxxxxxxx*@yahoo.com. *EC* is a Facebook subscriber under the name "Eric Makesumoutofnuttin Carter", User ID: 155832940.

10. An Internet Protocol address (IP address) is a numerical label assigned to each device connected to the public internet. Typically, the IP address is assigned to a computer by an Internet Service Provider (ISP) that has been contracted by a subscriber for the purpose of providing internet access. The assigned IP address associates the subscriber to the device which is connected to the internet.

11. It is possible for someone to hide their IP address, and thus their true location, when utilizing the internet. An anonymous proxy server, sometimes called a web proxy, generally attempts to anonymize web surfing. When someone utilizes a web proxy, the destination server (the server that ultimately satisfies the web request) receives the request from the anonymizing proxy server, and thus does not receive information about the end user's actual IP address. Anonymous proxy servers are located throughout the world and can be used to make

a subscriber's internet activities appear to be from an IP address not associated with the user, which may be located in another city, state or country. There are many websites that provide this service for free; including http://www.azproxies.com.

12. On or about February 29, 2012, a person posing as *EC* used a computer or similar device to send the below electronic communication via the Internet to the Austin Police Department ("APD") Public Information Officer:

From:	*ec* [mailto:l*xxxxx*e@gmail.com]
Subject:	My address is 6700 *sd* austin texas 78*xxx* {sic}
Message:	This message is from *ec*. I am going to kill everybody at austin high school I am also going to kill every policr I see {sic}

13. On or about March 1, 2012, a person posing as *EC* used a computer or similar device to send the below electronic communication via the Internet to the APD Public Information Officer:

From:	*Ec* [mailto:l*xxx*@yahoo.com]
Subject:	I am going to kill the barack obama and the austin police {sic}
Message:	This message is from *Ec*. I am going to kill every police I see and barack obama my name is *ec* my address is 6700 *sd* austin texas 78*xxx* {sic}

14. On or about March 2, 2012, a person posing as *EC* used a computer or similar device to send the below electronic communication via the Internet to the APD Public Information Officer:

From:	*Ec* [mailto:l*xxx*@yahoo.com]
Subject:	I am going to kill barack obama and every cop I see {sic}
Message:	This message is from *Ec*. I am going to blow up lbj high school I am going to kill the police chief I am also going to kill barack obama I have bombs and guns at my house my name id *ec* my date if birth is *xxxxxxxxxxxxx*[1] my address is 6700 sd austin texas {sic}

1 The date of birth given in this electronic communication matched the date of birth of the real individual, *EC*.

15. On or about March 2, 2012, a person posing as *EC* used a computer or similar device to send the following electronic communication via the Internet to the Royal Canadian Mounted Police ("RCMP"):

Topic:	Firearms
Comments:	I am going to kill the canda president I am also going to kill predident barack obama I am going to kill as many cops as I seen I am going to blow uo a plane my name is *ec* my address is 6700 *sd* Austin texas 78*xxx* {sic}
From:	*EC*
E-Mail:	L*xxxxxxxxxxxx*@yahoo.com
Telephone:	512-*xxx*-*xxx*8

16. On or about March 2, 2012, a person posing as *EC* used a computer or similar device to send the following electronic communication via the Internet to the White House:

From:	*EC*
Email:	L*xxxxxxxxxxxx*@yahoo.com
Phone:	
Address:	6700 *sd* Austin TX 78*xxx*
Topic:	Afghanistan & Iraq
Message:	I am going to kill barack obama and joe biden I will blow up a plane I have bombs and guns at my house I will kill every cop I see {sic}

17. On or about March 4, 2012, a person posing as *EC* used a computer or similar device to send the following electronic communication via the Internet to the Austin Independent School District ("AISD") Police Department:

Subject:	Anonymous Tip
From :	My name is *Kl*. My email address is –Email Not Given--.
Comments:	There is a guy name *ec* saying he is going to bring guns and bombs to school and kill lots of people his home address is 6700 *sd* austin texas 78*xxx* {sic}

18. On or about March 4, 2012, a person posing as *EC* used a computer or similar device to send the following electronic communication via the Internet to the AISD Police Department:

Subject:	Anonymous Tip
From :	My name is *Ma*. My email address is Lxxxxxxxxxxxx@yahoo.com.
Comments:	There is a student at austin high sais on Tuesday he is going to bring a gun to ausyin high school and kill a lot of student he has bomb and guns at his house his address is 6700 *sd* austin tx 78*xxx* {sic}

19. On or about March 4, 2012, the University of Texas ("UT") Police Department received a Text to Landline[2] voice message from telephone number 512-7*xx-xxx*5. The automated message said "There are two bombs hidden on campus and there will be a shooting by a student on Monday."

20. On or about March 4, 2012, the AISD Police Department received a Text to Landline voice message from telephone number 512-7xx-xxx5. The automated message said, "There is a student named *EC* saying he is going to shoot students on Tuesday at Austin High School."

21. On or about March 4, 2012, the UT Police Department determined through a confidential source that the following information regarding telephone number 512-7*xx-xxx*5:

Telephone Number:	512-7*xx-xxx*5
Subscriber Name:	*EC*
Address:	*6700 SD*, in Austin, TX
Date of Subscription:	December 6, 2011

2 "Text to Landline" allows the user to send text messages, which will be converted to voice, to any landline phone in the United States. The recipient's phone will ring and when it is answered the user's text message will be automatically read to them. If the recipient does not answer the phone your text message will be stored as voicemail. (Recipient must have a voicemail service on their landline.)

22. On or about March 5, 2012, the Pennsylvania State University Police received a Text to Landline voice message from telephone number 512-7*xx-xxx*5. The automated message said, "I am giving you a tip there are two bombs hidden in the bathroom, there is a student who is going to bring a gun and kill students."

23. On March 4, 2012 and March 5, 2012, the UT Police obtained a confidential source who provided that telephone number 512-7xx-xxx5 was being used at a physical address located on S*xxxxxxx* Lane in Austin Texas.

24. On March 5, 2012, APD reported that a resident of 1*xxx* S*xxxxxxx* Lane, in Austin, Texas called police on February 13, 2012 to report John Peter Bateman had threatened to kill himself and his mother. Austin Police responded to the scene and learned Bateman was angry with his mother because he was restricting from accessing the internet via his computer.

25. On March 5, 2012, additional criminal record checks revealed John Peter Bateman was previously convicted of stalking, in violation of Texas Penal Code Section 42.072, in 2010. Bateman was currently on parole with the State of Texas. The records also revealed Bateman has a history of making false emergency reports to police.

26. On March 5, 2012, members of the USSS, APD, UT Police, and AISD Police responded to 1*xxx* S*xxxxxxx* Lane, Austin, Texas and interviewed John Peter Bateman. Bateman was advised of his rights per Miranda and agreed to answer questions. Bateman admitted he sent approximately thirty or more threatening communications to various local, state, federal, and international government entities while posing as *EC* or implicating *EC* in the carrying out of said threats.

27. Bateman admitted he possesses and uses computers and telephones which can access the internet. Bateman admitted he utilized one or more of these instruments to make

threats by electronically communicating with various official government websites via the internet. Bateman admitted he made these threats utilizing a web proxy in an effort to disguise the fact he posted threatening messages on official government websites.

28. Bateman admitted he possesses and uses a cellular telephone assigned phone number 512-7*xx-xxx5*. Bateman admitted he utilized this cellular telephone to make threats by sending 'text to landline' messages to various educational institutions and law enforcement agencies. Bateman explained that he originally acquired and registered this cellular telephone in 2011 using the alias name of *JA* and that he later changed the registration of the phone to reflect the name *EC*.

29. Bateman admitted he electronically communicated one or more threats to kill the President of the United States and the President of Canada to the RCMP. Bateman admitted he electronically communicated one or more threats to kill the President of the United States to the White House. Bateman admitted he electronically communicated one or more threats to blow up LBJ High School in Austin, Texas to the APD. Bateman admitted he electronically communicated one or more threats to kill students at Austin High School to the AISD Police Department. Bateman admitted electronically communicating one or more messages claiming there were bombs hidden on the UT campus to the UT Police Department. Bateman admitted electronically communicating one or more messages claiming there were bombs hidden on the Pennsylvania State University campus to the Pennsylvania State University Police Department.

30. Bateman claimed he had never personally met *EC* or had any significant communication with him. Bateman claimed he somewhat indiscriminately 'meets' people on social networking websites. Bateman claimed he initially 'met' *EC* on MySpace a few years ago and recently discovered *EC's* Facebook page. Bateman claimed he and *EC* subsequently became

"Facebook Friends". Bateman claimed he noticed *EC's* Facebook page included one or more photos of *EC* posing with a large amount of money and with a gun. Bateman claimed he also noticed *EC* had personal information on posted his Facebook page; including *EC's* date of birth and physical address.

31. Bateman indicated he made the threatening communications primarily as a means to harass *EC*, however, he offered no substantive explanation as to why he targeted *EC* for harassment.

32. Bateman said he subscribed to Facebook under the alias name of "John Jones." Bateman said his Facebook page indicates he currently lives in Austin, TX and is originally from Temple, TX. I subsequently accessed the Facebook website and used the information provided by Bateman to locate his "John Jones" Facebook account. Bateman's association to the "John Jones" account was further confirmed by the presence of photographs of Bateman and of a vehicle registered to him. Examination of Bateman's "John Jones" Facebook account revealed Bateman has 58 "Facebook Friends," including *EC*.

CONCLUSION

33. Based on the foregoing facts and my training and experience, I have probable cause to believe that information retained by Facebook.com will aid in the investigation and prosecution of John Peter Bateman.

In view of the foregoing, your Affiant respectfully requests the Court issue a Search Warrant permitting the search and seizure of the electronically stored information relating to the following Facebook accounts:

"John Jones"
UID: 100002926201234
http://facebook.com/profile.php?id=100002926201234

and

"Eric Makesumoutofnuttin Carter"
UID: 155832940
http://facebook.com/profile.php?id=1558326940

This affidavit includes information which identifies the Facebook account of *EC*, a private citizen who is not a target of law enforcement investigation or suspected of any criminal wrongdoing. This information is made part of this affidavit and cannot be redacted because it is necessary to identify the specific Facebook account for which records are being sought. Public disclosure of this information would expose *EC* to further intrusions into his private life. In view of this, your affiant respectfully requests the Court issue an order to seal this search warrant and search warrant application/affidavit to protect the privacy of *EC*.

Respectfully submitted,

Andrew Dooher
Senior Special Agent
United States Secret Service

Subscribed and sworn before me
this 21st day of March, 2012

United States Magistrate Judge

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

IN RE SEARCH OF:	)	
	)	
FACEBOOK ACCOUNTS:	)	CASE NO.
	)	
"John Jones"	)	
Facebook UID: 100002926201234	)	
	)	
And	)	
	)	
"Eric Makesumoutofnuttin Carter"	)	
Facebook UID: 155832940	)	

ATTACHMENT A

LIST OF ITEMS TO BE SEIZED

I. SERVICE OF WARRANT AND COPYING OF FILES BY FACEBOOK

1. The officer executing this warrant shall affect service by any lawful method including faxing the warrant (with Facebook's consent) to Facebook's offices at the location specified in the warrant.

2. The officer executing this warrant shall permit Facebook, as custodian of the computer files described in Section II below, to locate the files, copy them onto removable electronic storage media or print them out as paper copies (or use a different copying method if specified in Section II below), and deliver the copies to the officer, who need not be present during this process at the location specified in the warrant.

II. COMPUTER FILES TO BE COPIED AND DELIVERED BY FACEBOOK

All records, photos and other stored information pertaining to the categories specified below, in whatever form kept, in the possession or control of Facebook.com Online Services ("Facebook"), headquartered at 18 Hacker Way, Menlo Park, CA 94025, relating to the account(s):

"John Jones"
UID: 100002926201234

http://facebook.com/profile.php?id=100002926201234

and

"Eric Makesumoutofnuttin Carter"
UID: 155832940
http://facebook.com/profile.php?id=1558326940

Such items to be seized should include, but not be limited to, the following:

(1) all subscriber information (including subscriber names, addresses, telephone numbers, screen names, account numbers, status of account, duration of account, and method of payment) for the owner or creator of this page;

(2) all account history (including customer Terms of Service and any complaints);

(3) all detailed billing records (including date, time, duration, and screen name used each time a particular account was activated);

(4) a complete log file of all activity relating to the page (including IP connection dates, times, method of connection, port, dial-up, and/or location);

(5) all records of subscriber account preferences, including, but not limited to, the name and Internet address of any "favorite places" or "book-marked" websites specified by the user(s) of the accounts, along with any "address books," "buddy lists," or "member profiles" maintained by, or related to, the account(s);

(6) all e-mail, including any attachments, sent by or received by the accounts, whether saved or deleted, whether contained directly in the e-mail account or in a customized "folder;"

(7) all images, photos and visual depictions, in any way associated with the account and in whatever form stored;

(8) all web-pages, including any posted images and associated links, that were created, maintained or accessed by the user(s) of the above-described account;

(9) all Privacy Preferences;

(10) all Calendar entries;

(11) all files saved to the Target Account's Facebook drive;

(12) any and all "Chat" accounts, and all information contained therein, associated

with the account; and

(13) any and all chat logs associated with the account.

Copies of the above-described records and stored information should be obtained from original storage and provided on CD-R (CD-Recordable) media.